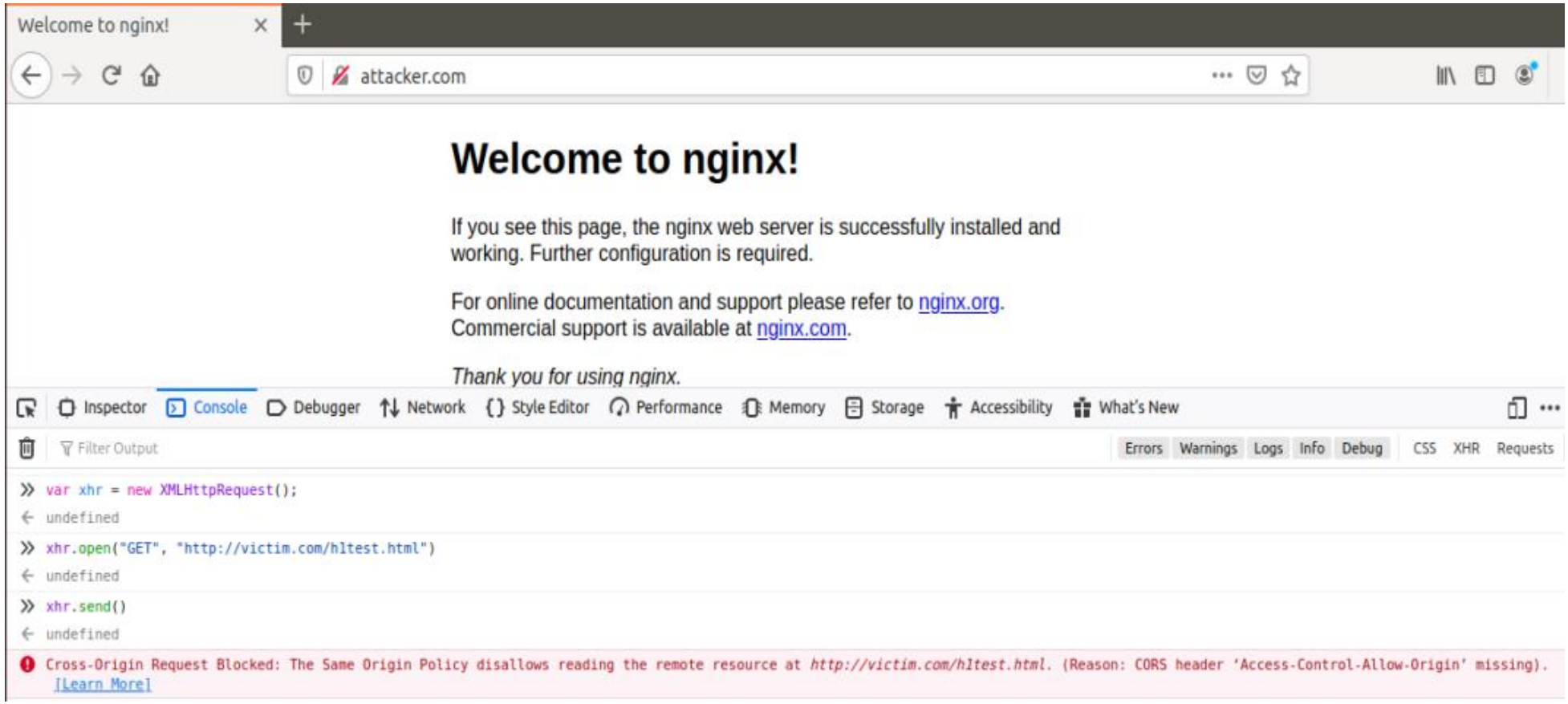
1. Откроем консоль браузера на странице http://attacker.com и запросим с помощью XHR файл с http://victim.com



Видим, что Same Origin Policy не позволяет нам этого сделать из-за заголовка Access-Control-Allow-Origin

2. Убеждаемся, что attacker.com и victim.com резолвятся в 127.0.0.1 (внесена соответствующая запись в файле hosts)

создаем файлы evil.js:

```
alert("I'm evil!");
```

и some.js:

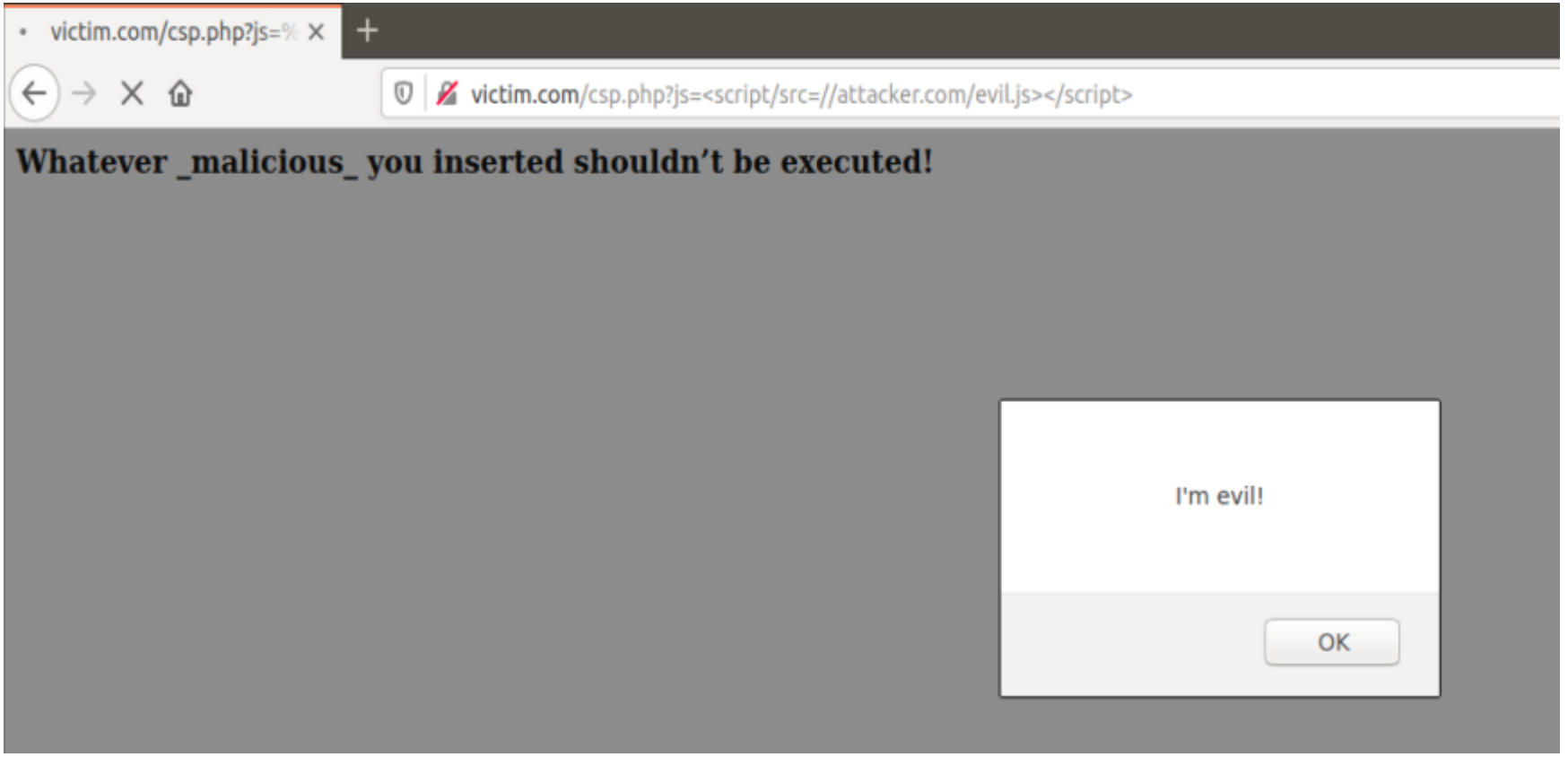
```
alert("I'm legitimate!");
```

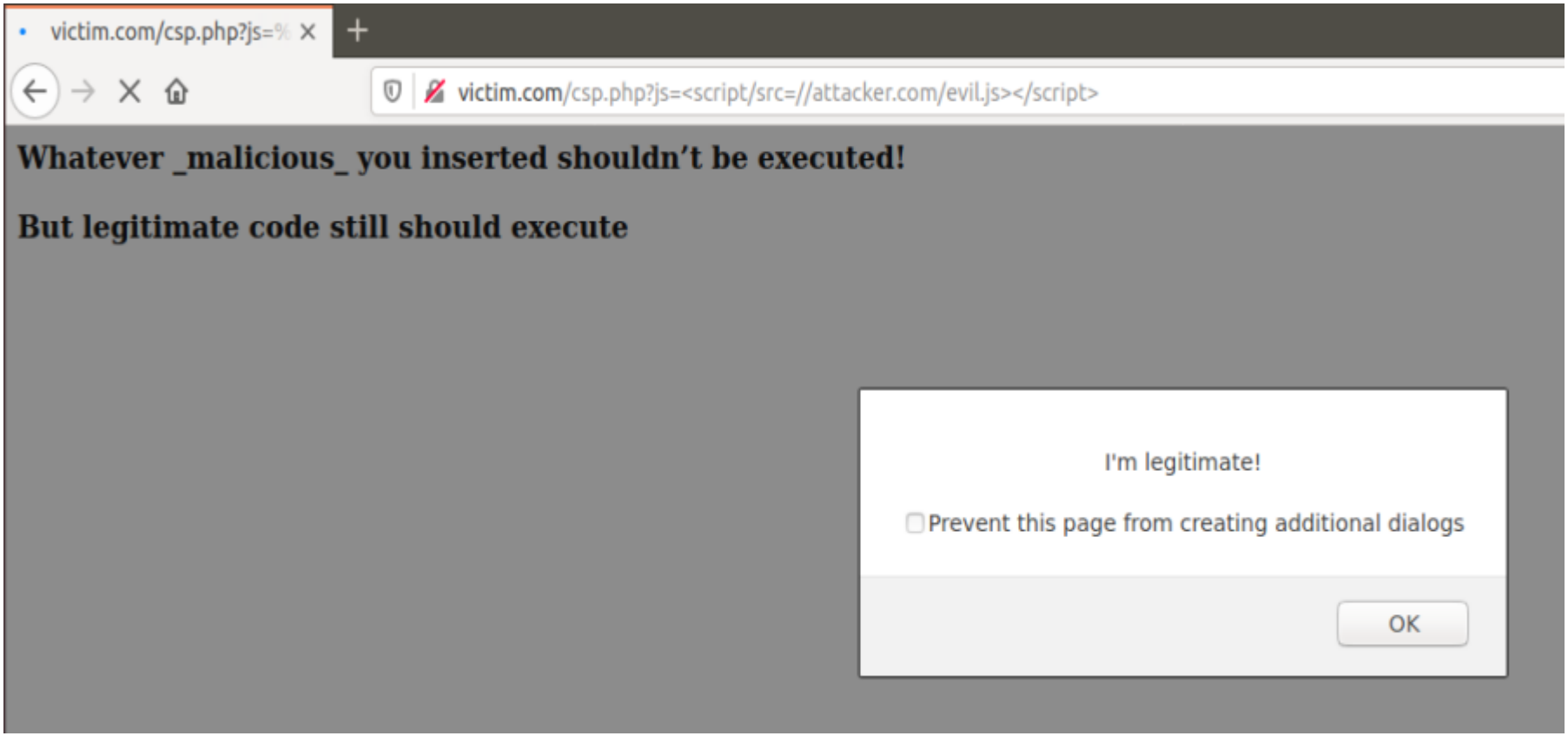
создаем файл csp.php:

```
<body>
  <h3>Whatever _malicious_ you inserted shouldn't be executed!</h3>
    <?php
      echo $_GET["js"];
    ?>
  <h3>But legitimate code still should execute</h3>
  <script src="http://victim.com/some.js"></script>
</body>
```

Проверяем работу алертов до изменения политики CSP

```
location ~ \.php$ {
        include snippets/fastcgi-php.conf;
#
#       # With php-fpm (or other unix sockets):
        add_header Content-Security-Policy "default-src 'none'; script-src 'unsafe-inline' http:;";
```

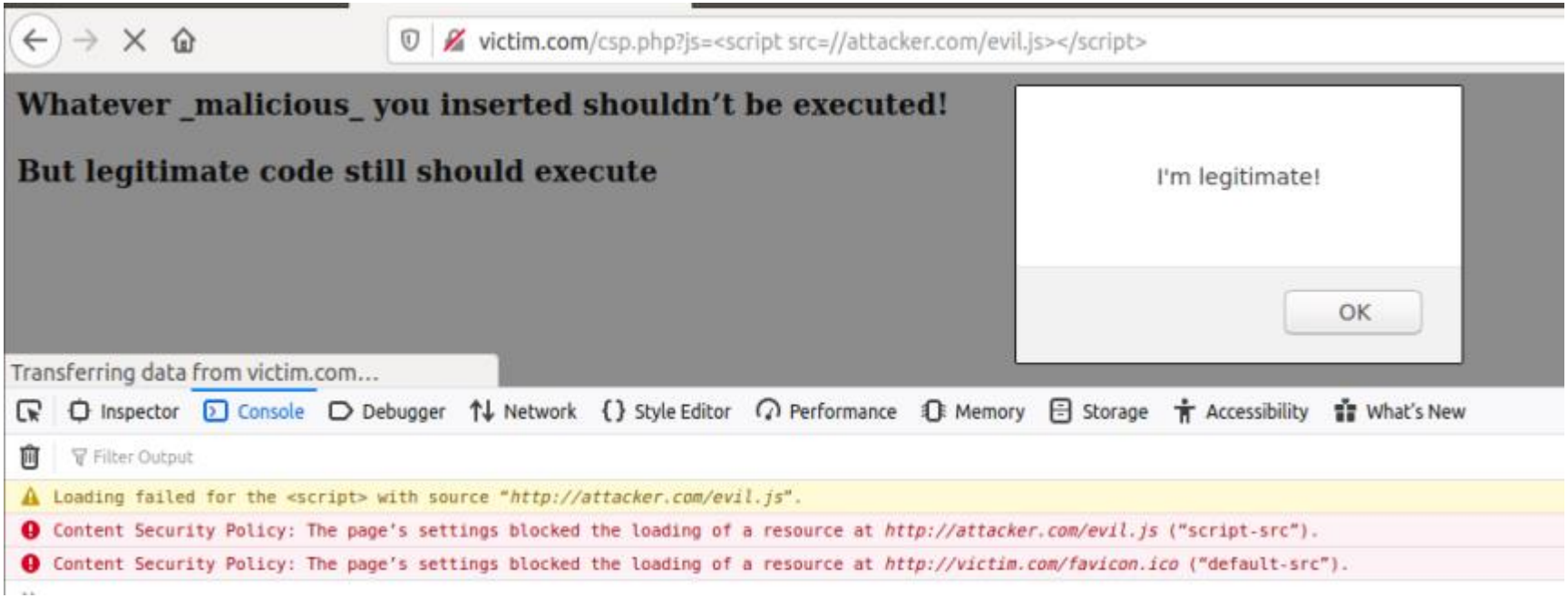




При такой политике срабатывают оба

Вносим изменения, чтобы вредоносный код не выполнялся (вносим в вайтлист доверенный домен)

```
location ~ \.php$ {
        include snippets/fastcgi-php.conf;
#
#       # With php-fpm (or other unix sockets):
        add_header Content-Security-Policy "default-src 'none'; script-src 'unsafe-inline' http://victim.com;";
```



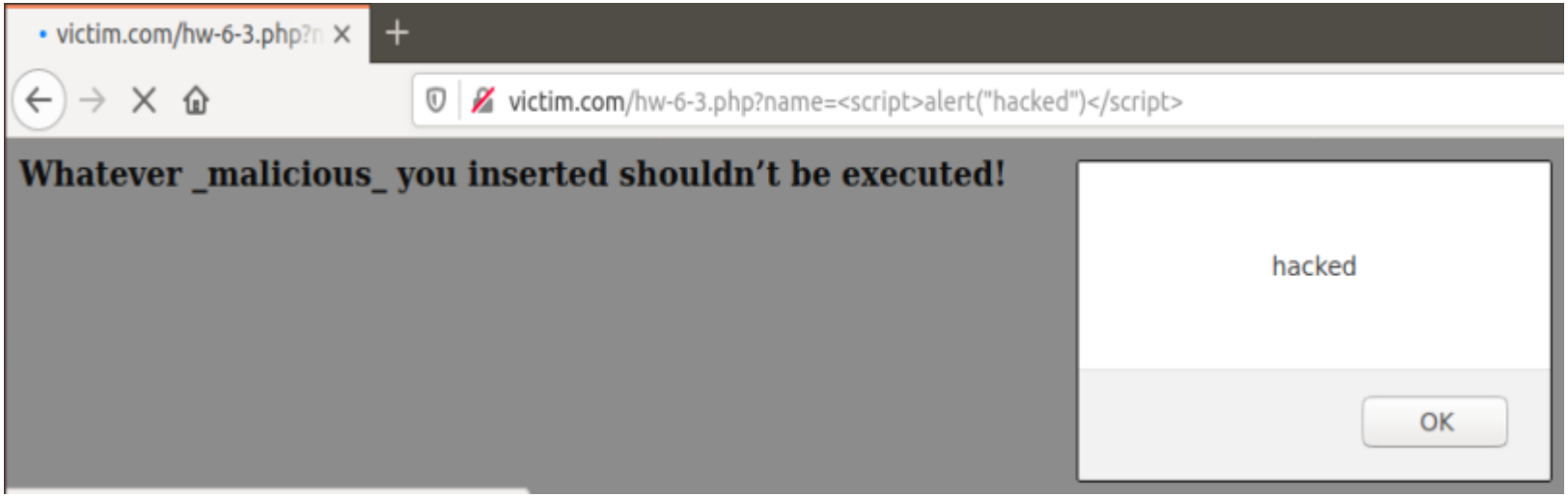
Чтобы обезопасить себя от инлайн скриптов, просто введенных в URL так же стоит убрать параметр unsafe-inline

```
location ~ \.php$ {
        include snippets/fastcgi-php.conf;
#
#       # With php-fpm (or other unix sockets):
        add_header Content-Security-Policy "default-src 'none'; script-src http://victim.com;";
```

3. Создаем файл hw-6-3.php

```
<body>
  <h3>Whatever _malicious_ you inserted shouldn't be executed!</h3>
  <?php
    echo $_GET["name"];
  ?>
  <h3>But legitimate code still should execute</h3>
  <script src="http://victim.com/some.js"></script>
  <script src="http://sub.victim.com/some.js"></script>
</body>
```

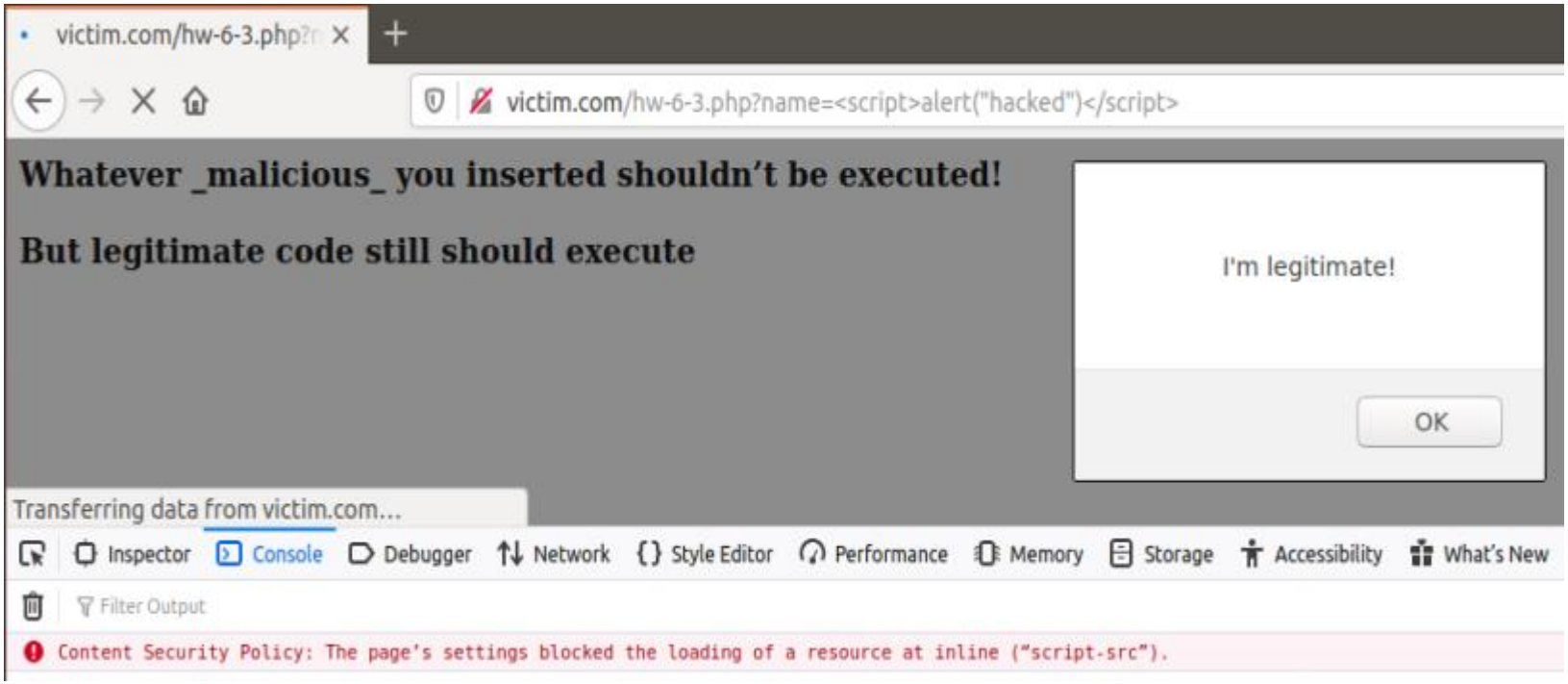
Он содержит XSS уязвимость



Для защиты от XSS в данном случае можно использовать nonce или hash. Используем nonce:

```
add_header Content-Security-Policy "script-src 'nonce-12345' http://victim.com http://sub.victim.com;";
```

В учебных целях зададим статичное значение (в работе настоящих сайтов используют случайно сгенерированные 256 битные числа, которые меняются при каждом новом запросе). Вредоносный скрипт заблокирован:



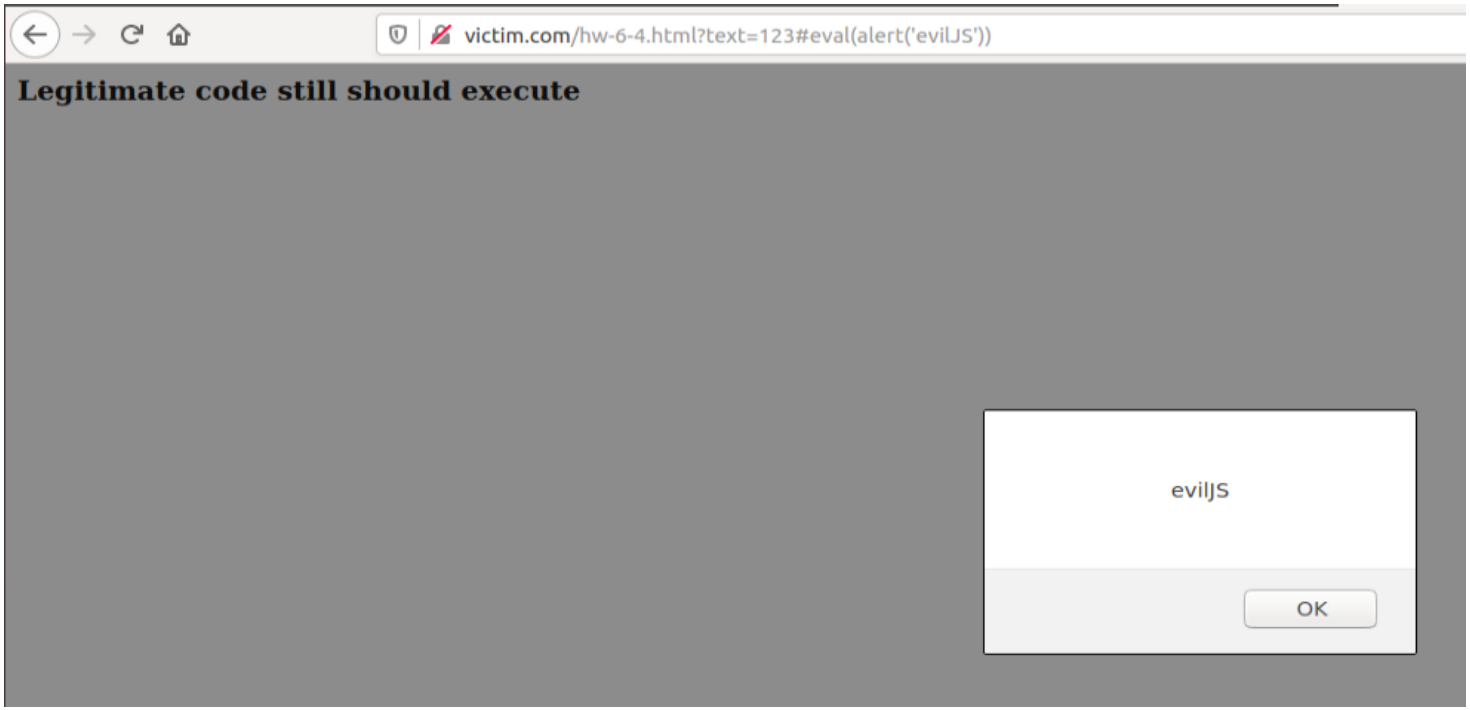
256 битные случайно сгенерированные числа, меняющиеся при каждом запросе, используются потому, что, если злоумышленник будет знать значение, то сможет выполнить вредоносный скрипт

4. Создаем файлы hw-6-4.html и hw-6-4.js

```
<body>
  <h3>Legitimate code still should execute</h3>
  <script src="/hw-6-4.js"></script>
</body>
```

```
function okFunction () {
  alert("I'm legitimate!");
}
setTimeout(document.URL.split("#")[1], 1000);
setTimeout(okFunction, 1000);
```

Обращаем внимание, что строчка `setTimeout(document.URL.split("#")[1], 1000);` в сочетании с политикой script-src ‘unsafe-eval’ позволяет из URL выполнить практически любую команду, например:



URL разбивается по разделителю “#” в массив строк и элемент с индексом 1 (т.е. 2-ой) выполняется с таймаутом 1 сек

Чтобы этого избежать, можно установить следующие настройки CSP, eval будет блокироваться браузером

```
add_header Content-Security-Policy "default-src 'self'; script-src http://victim.com http://partner.com;";
```

5. Установлен mySQL

```
flash@flash-VirtualBox:~/Загрузки$ sudo apt-get install mysql-server
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0
  grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-filesystem1.65.1 libboost-iostreams1.65.1
  libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcolamd2 libdazzle-1.0-0
  libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14
  libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4
  liblangtag-common liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1 libqqwing2v5
  libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxaplan30 libxmlsec1
  libxmlsec1-nss lp-solve media-player-info python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy
  usb-creator-common
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-client-core-5.7 mysql-common mysql-server-5.7
  mysql-server-core-5.7
Предлагаемые пакеты:
  libipc-sharedcache-perl mailx tinyca
Следующие НОВЫЕ пакеты будут установлены:
  libaio1 libevent-core-2.1-6 libhtml-template-perl mysql-client-5.7 mysql-client-core-5.7 mysql-common mysql-server
  mysql-server-5.7 mysql-server-core-5.7
Обновлено 0 пакетов, установлено 9 новых пакетов, для удаления отмечено 0 пакетов, и 49 пакетов не обновлено.
Необходимо скачать 159 kB/19,1 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 155 MB.
Хотите продолжить? [Д/н] y
Пол:1 http://ru.archive.ubuntu.com/ubuntu bionic/main amd64 mysql-common all 5.8+1.0.4 [7 308 B]
Пол:2 http://ru.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libaio1 amd64 0.3.110-5ubuntu0.1 [6 476 B]
Пол:3 http://ru.archive.ubuntu.com/ubuntu bionic/main amd64 libevent-core-2.1-6 amd64 2.1.8-stable-4build1 [85,9 kB]
Пол:4 http://ru.archive.ubuntu.com/ubuntu bionic/main amd64 libhtml-template-perl all 2.97-1 [59,0 kB]
Получено 159 kB за 0с (1 233 kB/s)
Предварительная настройка пакетов ...
Выбор ранее не выбранного пакета mysql-common.
(Чтение базы данных … на данный момент установлен 154681 файл и каталог.)
Подготовка к распаковке …/0-mysql-common_5.8+1.0.4_all.deb …
Распаковывается mysql-common (5.8+1.0.4) …
Выбор ранее не выбранного пакета libaio1:amd64.
Подготовка к распаковке …/1-libaio1_0.3.110-5ubuntu0.1_amd64.deb …
Распаковывается libaio1:amd64 (0.3.110-5ubuntu0.1) …
Выбор ранее не выбранного пакета mysql-client-core-5.7.
Подготовка к распаковке …/2-mysql-client-core-5.7_5.7.29-0ubuntu0.18.04.1_amd64.deb …
Распаковывается mysql-client-core-5.7 (5.7.29-0ubuntu0.18.04.1) …
Выбор ранее не выбранного пакета mysql-client-5.7.
Подготовка к распаковке …/3-mysql-client-5.7_5.7.29-0ubuntu0.18.04.1_amd64.deb …
Распаковывается mysql-client-5.7 (5.7.29-0ubuntu0.18.04.1) …
Выбор ранее не выбранного пакета mysql-server-core-5.7.
Подготовка к распаковке …/4-mysql-server-core-5.7_5.7.29-0ubuntu0.18.04.1_amd64.deb …
Распаковывается mysql-server-core-5.7 (5.7.29-0ubuntu0.18.04.1) …
```

Создан пользователь bug

```
flash@flash-VirtualBox:~/Загрузки$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE USER 'bug'@'localhost' IDENTIFIED BY 'bug';
Query OK, 0 rows affected (0.01 sec)
```

Пробуем подключиться

```
flash@flash-VirtualBox:~/Загрузки$ mysql -u bug -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

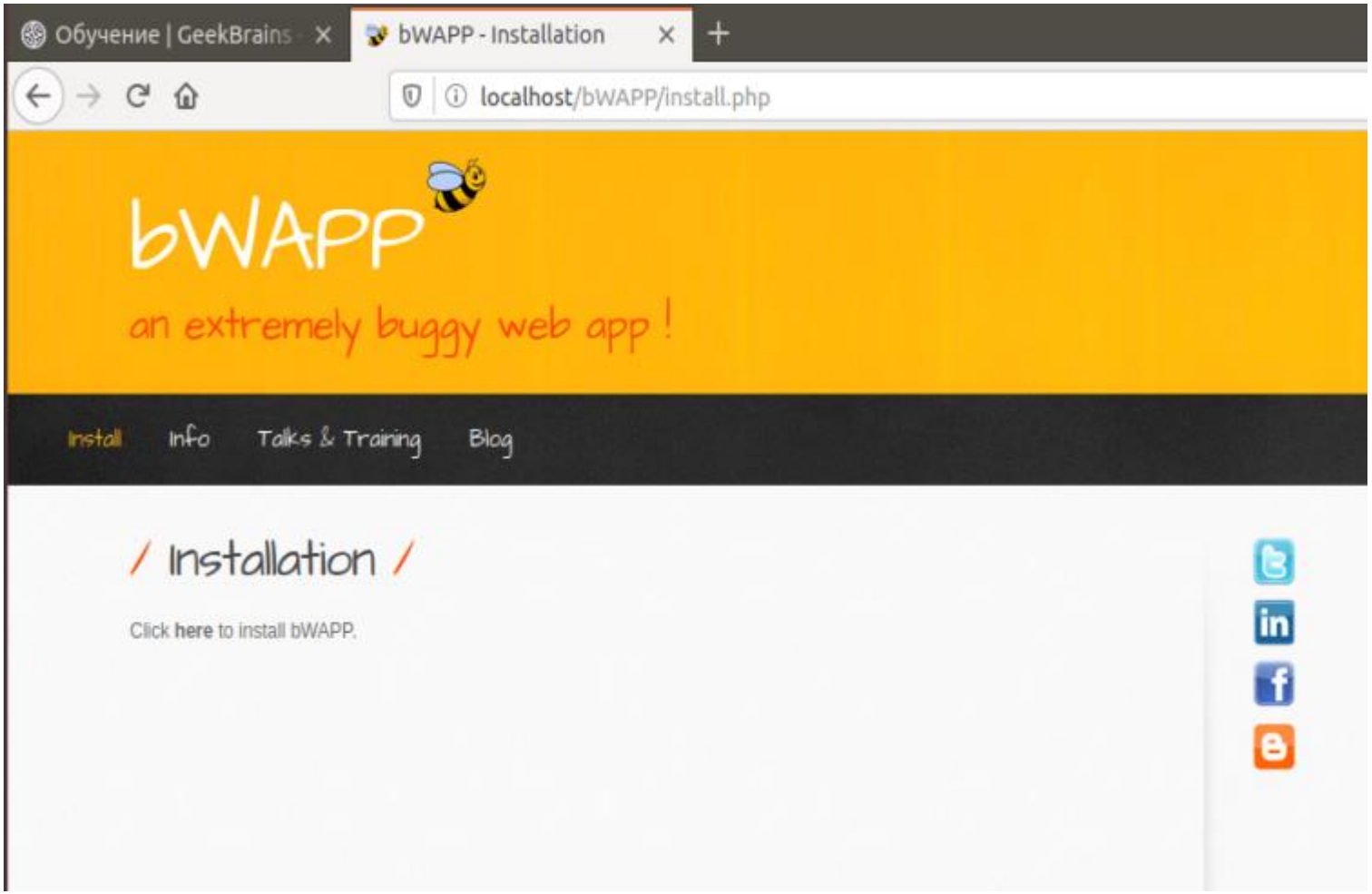
В настройках bWAPP (/var/www/html/bWAPP/admin/settings.php) указываем данные пользователя и название базы

```
$db_server = "localhost";
$db_username = "bug";
$db_password = "bug";
$db_name = "bWAPP";
```

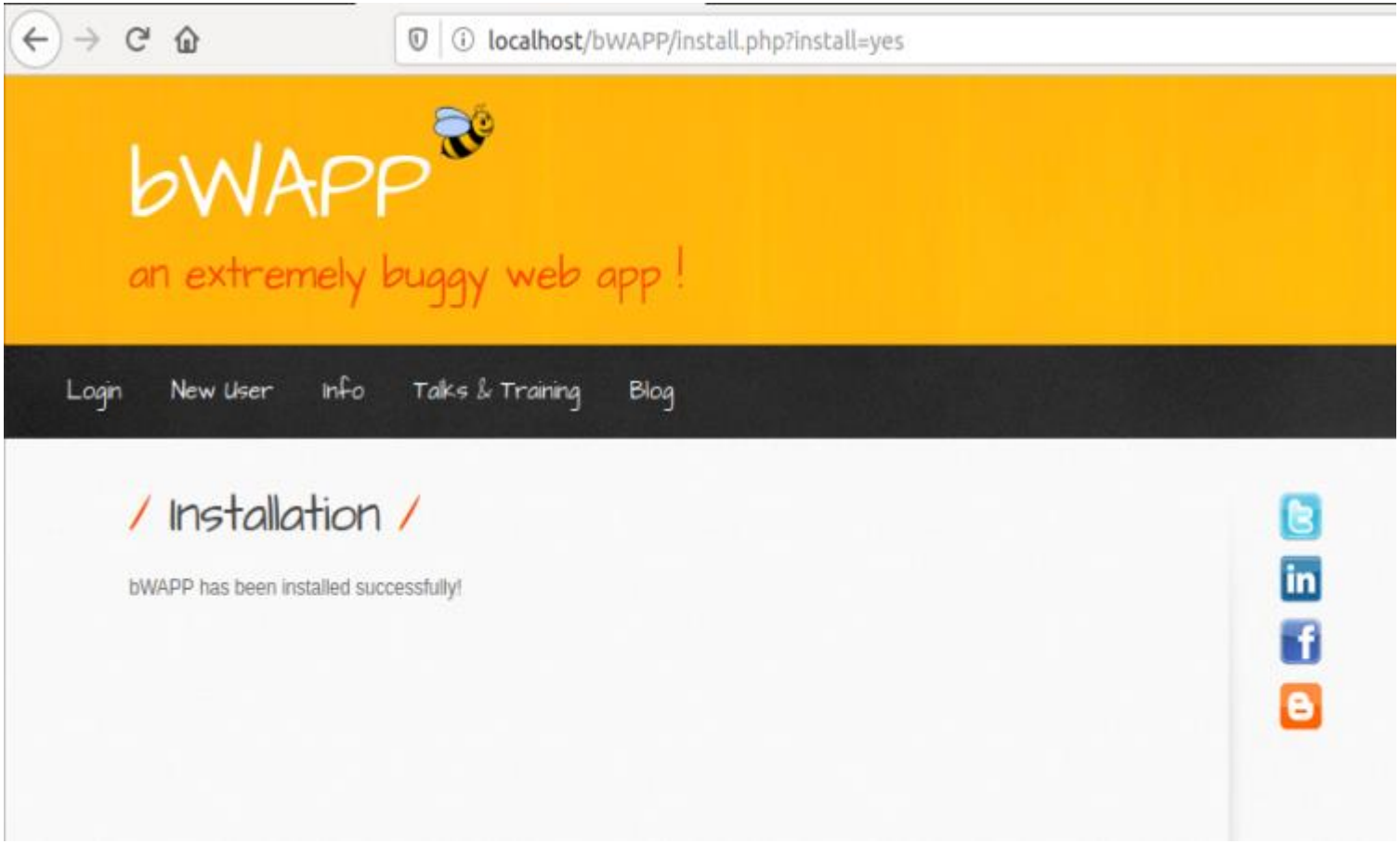
Выдаем права директориям

```
flash@flash-VirtualBox:/var/www/html/bWAPP$ sudo chmod 777 passwords/
flash@flash-VirtualBox:/var/www/html/bWAPP$ sudo chmod 777 images/
flash@flash-VirtualBox:/var/www/html/bWAPP$ sudo chmod 777 documents/
flash@flash-VirtualBox:/var/www/html/bWAPP$ sudo chmod 777 logs/
```

Переходим по адресу localhost/bWAPP/install.php

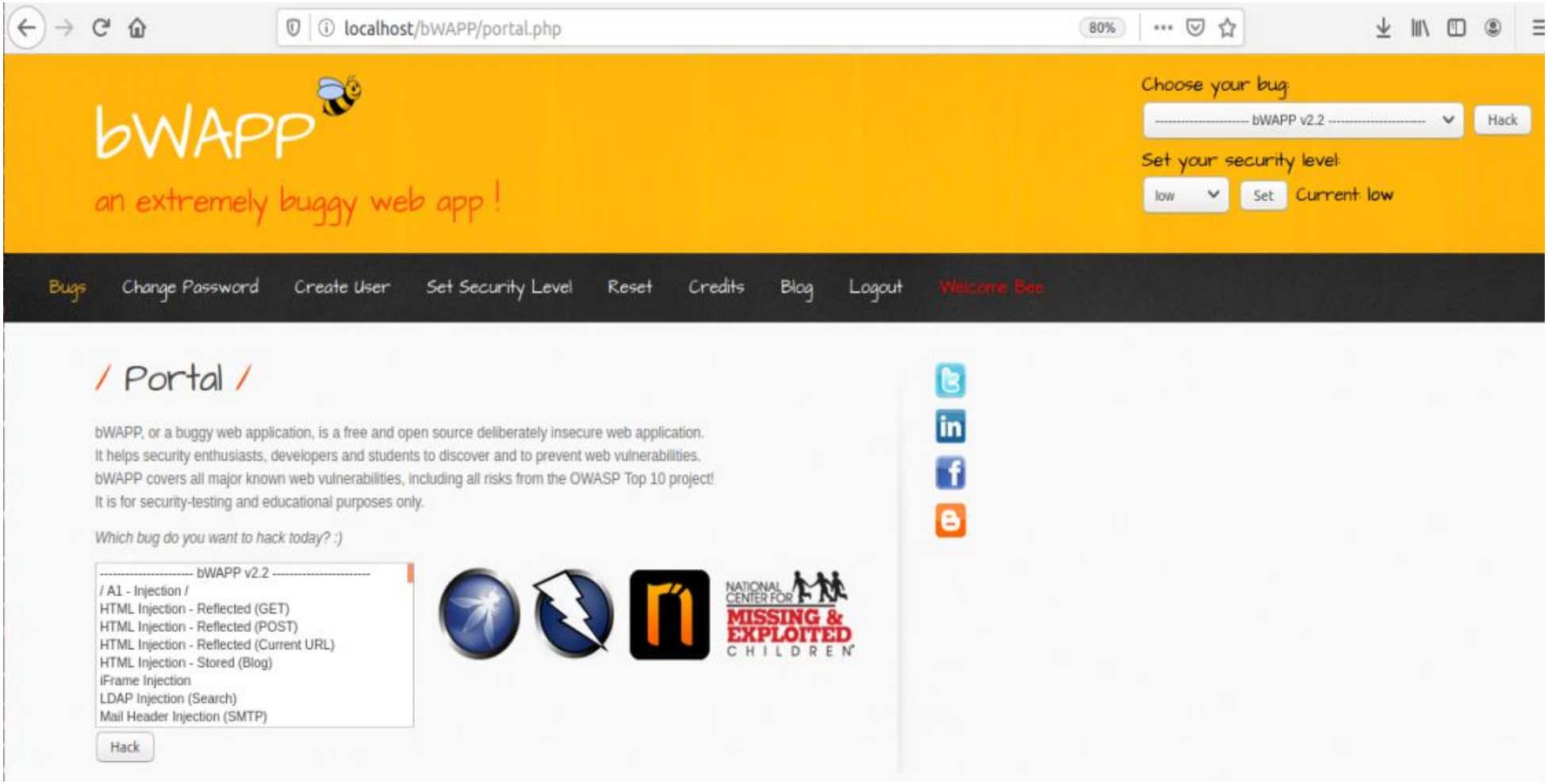


Жмем here


localhost/bWAPP/install.php?install=yes
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Installation /
bWAPP has been installed successfully!

Логинимся


localhost/bWAPP/login.php
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Login /
Enter your credentials (bee/bug).
Login:
bee
Password:
Set the security level:
low
Login
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
with
netsparker
Web Security Scanner


localhost/bWAPP/portal.php
80%
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ Portal /
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.
Which bug do you want to hack today? :)
---------- bWAPP v2.2 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN